REMARKS

The present application and its claims are directed to a mobile application security system and method.

MINOR DEFICIENCIES

Applicant is resubmitting, with an Information Disclosure Statement with this response, a 1449 form that includes the U.S. patents previously submitted in April 2002.

DOUBLE PATENTING

In response to the Examiner's rejection of Claims 1-20 under the judicially created doctrine of obviousness-type double patenting over Claims 1-20 of U.S. Patent Application Serial No. 09/764,548, this rejection should be a provisional rejection as both application are pending and no claims have been allowed. Applicant will consider the submission of a terminal disclaimer, if and when the claims in this application are allowable.

PRIOR ART REJECTIONS

In response to the Examiner's rejection of Claims 1-20 under 35 U.S.C. 102(a) as being anticipated by Jansen et al., NIST Special Publication 800-19- Mobile Application Security (hereinafter "Jansen"), Applicant respectfully traverses the rejection. In particular, the claims are not anticipated by Jansen, for the reasons set forth below, and early allowance of the claims is respectfully requested.

Claims 1 and 11

Claim 1 is not anticipated by Jansen for at least the reason that Jansen does not disclose "the central computer further comprising means for monitoring the security of the mobile application as it jumps between the host computers wherein when the mobile application is communicated from a first host to a second host, it passes through the central computer" as set forth in the claim. To support his rejection, the Examiner cites to pages 18-19. At pages 18-19, Jansen, citing to the Jumping Beans system, describes a system with a secure central host and a decentralized system called Aglets wherein each host is capable of rejecting an agent from a platform that is not a trusted peer. Clearly, the Aglets system does not have a central computer. The Jumping Beans systems as described in the Jansen article, has a secure central host, but Jansen does not describe that the Jumping Beans system performs the operations set forth in the

claim, namely the security monitoring of the mobile application at the central computer when the mobile application is communicated from a first host to a second host.

Section 4.2 of Jansen (on pages 18-19) describes the problem of protecting an agent which "stems from the inability to effectively extend the trusted environment of an agent's home platform to other agent platforms." See page 18, second paragraph. For the reasons that the claimed system has the central computer through which the mobile application is communicated, the claimed system does not suffer from this drawback highlighted by Jansen. In fact, this section makes it clear that Jansen is describing a mobile application system in which each host platform performs its own security. Thus, Section 4.2 of Jansen does not in any way disclose or suggest a system with a central computer that performs security monitoring. Thus, Jansen does not teach this element of Claim 1.

In addition, Claim 1 is not anticipated by Jansen for the reason that Jansen does not disclose "the security monitoring means further comprises means for detecting unwanted changes in the code associated with the mobile application when the mobile application is jumping between hosts." The Examiner has cited Sections 2.2.4 and 2.3.4 of Jansen to support his rejection of this element of Claim 1. Section 2.2.4 teaches that the modification of an agent's code is a particularly insidious form of attack. Jansen also describes using signed code to solve this problem. However, the signed code described in Jansen does not permit a trusted host to modify the code of a mobile application (as it might do), requires each host to maintain a list of the trusted hosts and requires the secure distribution of the public keys. This signed code is not a central computer that monitors the security of the mobile application.

Section 2.3.4 of Jansen teaches that a platform must be prevented from modifying an agent's code, state or data without being detected and describes some examples of this problem. Jansen also describes that an original author can sign the agent's code to prevent changes in the code. Jansen then describes that a multi-hop scenario is more risky than a single hop problem. Thus, in Section 2.3.4, Jansen teaches 1) that code modification is bad; 2) that a digital signature may prevent some code modification; and 3) that multi-hop risks are higher since the mobile application is farther away from its home platform. Thus, Jansen describes the problem, but one again does not offer any solution to the problem. Furthermore, nothing in Jansen teaches or suggests that a central computer detects unwanted changes in the code associated with the mobile

application when the mobile application is jumping between hosts as set forth in the claim. Thus, Jansen does not disclose or suggest the invention recited in Claim 1. Claim 11 are allowable over Jansen for at least the same reasons as Claim 1.

Claims 2 and 12

Claim 2 is allowable for at least the same reasons as Claim 1 above. In addition, Claim 2 is not anticipated by Jansen as Jansen does not teach that a central computer stores a copy of a mobile application and then compares it to the mobile application after execution by another host as set forth in the claim. To support the rejection, the Examiner cited in Section 3.2 of Jansen and states "1st paragraph teaches protecting against modification of code, ie. comparing the original to the one received." However, the second portion of the statement by the Examiner does not logically follow from the first part as there are many different ways to protect against code modification and the first statement does not in any way imply or suggest the conclusion made by the Examiner. Therefore, there is no support in Section 3.2 for the Examiner's rejection.

Furthermore, the Examiner has relied on Section 4.2.2 of Jansen that discusses mutual itinerary recording to support his rejection. However, Section 4.2.2 describes that the itinerary of the mobile agent is recorded by another agent and used to detect malicious platform behavior. However, this section of Jansen does not describe that the copy of the mobile agent (which is different from the itinerary) is made and then the stored copy may be compared to a mobile application from another host. Jansen's system attempts to catch inconsistencies in the itineraries of the mobile agents, but would not detect other code modifications of the mobile agent. In addition, the system in Jansen does not describe that the elements set forth in this claim are at the central computer as claimed.

Finally, the Examiner cites to the lists/tables at the bottom of page 14 and at the top of page 19 in Jansen to support his rejection of this claim. However, none of the items listed on page 14 or page 19 disclose (or even suggest) that a central computer stores a copy of a mobile application and then compares it to the mobile application after execution at another host as set forth in the claim. It is hard to imagine how one of ordinary skill in the art would use the claimed mobile application comparison element when it is not even suggested in the Jansen

article. Thus, the lists do not support the Examiner rejection of this claim and Claim 2 is allowable over Jansen.

Similarly, Claim 12 is allowable over Jansen for at least the same reasons as Claim 1 and is further allowable over Jansen for at least the same reasons as Claim 2 above.

Claim 3

Claim 3 is not anticipated by Jansen for at least the same reason as Claim 1.

Claims 4 and 13

Claim 4 is not anticipated by Jansen for at least the reason that Jansen does not disclose "the central computer further comprising means for monitoring the security of the mobile application as it jumps between the host computers wherein when the mobile application is communicated from a first host to a second host, it passes through the central computer" as set forth in the claim. To support his rejection, the Examiner cites to pages 18-19. At pages 18-19, Jansen, citing to the Jumping Beans system, describes a system with a secure central host and a decentralized system called Aglets wherein each host is capable of rejecting an agent from a platform that is not a trusted peer. Clearly, the Aglets system does not have a central computer. The Jumping Beans systems as described in the Jansen article, has a secure central host, but Jansen does not describe that the Jumping Beans system performs the operations set forth in the claim, namely the security monitoring of the mobile application at the central computer when the mobile application is communicated from a first host to a second host.

Section 4.2 of Jansen (on pages 18-19) describes the problem of protecting an agent which "stems from the inability to effectively extend the trusted environment of an agent's home platform to other agent platforms." See page 18, second paragraph. For the reasons that the claimed system has the central computer through which the mobile application is communicated, the claimed system does not suffer from this drawback highlighted by Jansen. In fact, this section makes it clear that Jansen is describing a mobile application system in which each host platform performs its own security. Thus, Section 4.2 of Jansen does not in any way disclose or suggest a system with a central computer that performs security monitoring. Thus, Jansen does not teach this element of Claim 4.

In addition, Jansen does not teach "wherein the security monitoring means further comprises means for preventing a host from transmitting hostile code in a mobile application to

another host." The Examiner has cited to IBM Aglets discussion on page 19 of Jansen to support his rejection of this element of the claim. However, it is clear from the description that the Aglets system does not have a central computer and that the Aglets system does not have a central computer that prevents a host from transmitting hostile code in a mobile application to another host. Furthermore, in the Aglets system, each host must block the mobile application which is different from a central computer performing that task. In addition, the Aglets system does not prevent a host from transmitting the hostile code as claimed, but only blocks the mobile application at a particular host.

Furthermore, for the reasons that the claimed system has the central computer through which the mobile application is communicated, the claimed system does not suffer from this drawback highlighted by Jansen. In fact, this section makes it clear that Jansen is describing a mobile application system in which each host platform performs its own security. Thus, Section 4.2 of Jansen does not in any way disclose or suggest a system with a central computer that performs security monitoring. Therefore, Claim 4 is allowable over Jansen. Claim 13 is allowable over Jansen for at least the same reasons as Claim 4.

Claims 5 and 14

Claim 5 is allowable over Jansen for at least the same reasons as Claim 4. In addition, Jansen does not disclose "means for stripping the code from an initially received mobile application if the host is not trusted, means for saving the code of the mobile application, and means, when requested by another host, for providing the code for the mobile application to the requesting host" as set forth in the claim. The Examiner asserts that Jansen discloses the claimed "stripping of code" since Jansen teaches identifying a non-trusted machine and many options exist to stay safe from the machine. However, the Examiner never cites to a portion of Jansen that discloses the specific element set forth in Claim 5. In fact, Jansen does not disclose the elements recited in Claim 5 and therefore Claim 5 is allowable over Jansen.

Claim 14 is allowable for at least the same reasons as Claim 5.

Claims 6 and 15

Claim 6 is not anticipated by Jansen for at least the reason that Jansen does not disclose "the central computer further comprising means for monitoring the security of the mobile application as it jumps between the host computers wherein when the mobile application is

communicated from a first host to a second host, it passes through the central computer" as set forth in the claim. As with the other independent claims, the Examiner may cite to pages 18-19. At pages 18-19, Jansen, citing to the Jumping Beans system, describes a system with a secure central host and a decentralized system called Aglets wherein each host is capable of rejecting an agent from a platform that is not a trusted peer. Clearly, the Aglets system does not have a central computer. The Jumping Beans systems as described in the Jansen article, has a secure central host, but Jansen does not describe that the Jumping Beans system performs the operations set forth in the claim, namely the security monitoring of the mobile application at the central computer when the mobile application is communicated from a first host to a second host.

Section 4.2 of Jansen (on pages 18-19) describes the problem of protecting an agent which "stems from the inability to effectively extend the trusted environment of an agent's home platform to other agent platforms." See page 18, second paragraph. For the reasons that the claimed system has the central computer through which the mobile application is communicated, the claimed system does not suffer from this drawback highlighted by Jansen. In fact, this section makes it clear that Jansen is describing a mobile application system in which each host platform performs its own security. Thus, Section 4.2 of Jansen does not in any way disclose or suggest a system with a central computer that performs security monitoring. Thus, Jansen does not teach this element of Claim 6.

In addition, Claim 6 is not anticipated by Jansen for the reason that Jansen does not disclose "the security monitoring means further comprises means for detecting unwanted changes in the state associated with the mobile application when the mobile application is jumping between hosts." The Examiner cites Section 4.1.4 ("State Appraisal") to support his rejection of this claim. Section 4.1.4 discusses the desire to detect changes in the state of the mobile application. Section 4.1.4 further describes a system in which the owner and author is an agent may generated an appraisal function that becomes part of the agent's code. The appraisal function permits an agent platform (the computer in Jansen most similar to the claimed host computer) to verify the correct state of an incoming agent and to determine the privileges that the agent can possess during execution. See second paragraph, third sentence of Section 4.1.4. Thus, Jansen discloses a system in which each agent platform (host computer) must perform its own state appraisal based on the appraisal functions in the code. In contrast, the claimed system

uses the central computer that performs the process of detecting unwanted changes in the state of the mobile application so that no appraisal function is required and each agent platform does not need to use an appraisal function. Thus, Section 4.1.4 does not disclose a central computer that detected unwanted changes in the state of a mobile application when the mobile application is jumping between hosts as claimed and Jansen does not anticipate Claim 6. Claim 15 is allowable over Jansen for at least the same reasons as Claim 6.

Claims 7 and 16

Claim 7 is allowable for at least the same reasons as Claim 6 above. In addition, Claim 7 is not anticipated by Jansen as Jansen does not teach that a central computer stores a copy of the state of the mobile application and then compares the state to a state of the mobile application after execution by another host as set forth in the claim. The Examiner has relied on page 17 (Sections 4.1.4 and 4.1.5) of Jansen to support his rejection of this claim. For the reasons set forth above for Claim 6, Section 4.1.4 does not support the rejection of this claim and furthermore does not disclose the elements set forth in Claim 7.

Section 4.1.5 of Jansen ("Path Histories") also does not support the Examiner's rejection of this claim. The path histories are a way to maintain an authenticable record of the prior platforms visited by an agent and requires that each agent platform to add a signed entry to the path. Jansen notes that a drawback of the path histories is that path verification becomes costly as the path history increases. As with Section 4.1.4 above, it is clear that Jansen contemplates a system in which each agent platform must perform security monitoring so that a next agent platform uses the path history in the agent to verify the past stops of the agent. See Section 4.1.5, the sentence that starts "Upon receipt". In contrast, the claimed system uses the central computer that performs the process of storing the state of a mobile application and then comparing the stored state to the state of the mobile application after execution by another host and does not need to generate or maintain the path history described in Jansen. Thus, Section 4.1.5 does not disclose the elements recited in Claim 7 and Claim 7 is allowable of Jansen. Similarly, Claim 16 is allowable over Jansen for at least the same reasons as Claim 7.

Claims 8- 10 and 17-19

Claim 8 is not anticipated by Jansen for at least the reason that Jansen does not disclose "the central computer further comprising means for monitoring the security of the mobile

application as it jumps between the hosts wherein data about the mobile application is communicated to the central computer when the mobile application is communicated from a first host to a second host" as set forth in the claim. To support his rejection, the Examiner cites to pages 18-19. At pages 18-19, Jansen, citing to the Jumping Beans system, describes a system with a secure central host and a decentralized system called Aglets wherein each host is capable of rejecting an agent from a platform that is not a trusted peer. Clearly, the Aglets system does not have a central computer. The Jumping Beans systems as described in the Jansen article, has a secure central host, but Jansen does not describe that the Jumping Beans system performs the operations set forth in the claim, namely the security monitoring of the mobile application at the central computer when the mobile application is communicated from a first host to a second host.

Section 4.2 of Jansen (on pages 18-19) describes the problem of protecting an agent which "stems from the inability to effectively extend the trusted environment of an agent's home platform to other agent platforms." See page 18, second paragraph. For the reasons that the claimed system has the central computer through which the mobile application is communicated, the claimed system does not suffer from this drawback highlighted by Jansen. In fact, this section makes it clear that Jansen is describing a mobile application system in which each host platform performs its own security. Thus, Section 4.2 of Jansen does not in any way disclose or suggest a system with a central computer that performs security monitoring. Thus, Jansen does not teach this element of Claim 8.

In addition, Claim 8 is not anticipated by Jansen for the reason that Jansen does not disclose "the security monitoring means further comprises means for detecting unwanted changes in the itinerary associated with the mobile application when the mobile application is jumping between hosts." The Examiner has cited Sections 4.2.2 and 4.2.4 of Jansen to support his rejection of this element of Claim 8. Section 4.2.2 describes multiple itinerary recording in which an agent's itinerary is recorded and tracked by another cooperating agent so that the peer (the cooperating agent) maintains a record of the itinerary and takes appropriate action when inconsistencies are noted. Although this section describes the notion of itinerary recording, it does not describe or suggest a central computer that performs detection of unwanted changes in the itinerary associated with the mobile application when the mobile application is jumping between hosts as set forth in the claim. Furthermore, the claimed system does not need to utilize

the mutual itinerary recording described in Jansen. Thus, this section does not support the rejection of this claim.

Section 4.2.4 ("Execution Tracing") describes a technique for detecting unauthorized modifications of an agent through the faithful recording of the agent's behavior during its execution on each agent platform. The technique requires "each platform involved to create and retain a non-repudiatable log or trace of the operations performed by the agent which resident there and to submit a cryptographic hash of the trace upon conclusion as a trace summary or fingerprint." See first paragraph, second sentence of Section 4.2.4. As above, this technique relies on each agent platform to perform security monitoring and, for this technique, generate the trace log. In contrast, the claimed system uses the central computer that comprises means for detecting unwanted changes in the itinerary of the mobile application so that the trace log of Jansen is not required and the claimed hosts do not need to generate the trace logs. Thus, Section 4.2.4 does not disclose a central computer that detects unwanted changes in the itinerary of a mobile application when the mobile application is jumping between hosts as claimed and Jansen does not anticipate Claim 8. Claims 9 and 10 are allowable over Jansen for at least the same reasons as Claim 8. Furthermore, Claim 17 is allowable for at least the same reasons as Claim 8 and Claims 18-19 are allowable for at least the same reasons as Claims 9-10.

Claim 20

Claim 20 is not anticipated by Jansen for at least the reason that Jansen does not disclose "the central computer further comprising means for monitoring the security of the mobile application as it jumps between the hosts wherein data about the mobile application is communicated to the central computer when the mobile application is communicated from a first host to a second host" as set forth in the claim. To support his rejection, the Examiner cites to pages 18-19. At pages 18-19, Jansen, citing to the Jumping Beans system, describes a system with a secure central host and a decentralized system called Aglets wherein each host is capable of rejecting an agent from a platform that is not a trusted peer. Clearly, the Aglets system does not have a central computer. The Jumping Beans systems as described in the Jansen article, has a secure central host, but Jansen does not describe that the Jumping Beans system performs the operations set forth in the claim, namely the security monitoring of the mobile application at the central computer when the mobile application is communicated from a first host to a second host.

Section 4.2 of Jansen (on pages 18-19) describes the problem of protecting an agent which "stems from the inability to effectively extend the trusted environment of an agent's home platform to other agent platforms." See page 18, second paragraph. For the reasons that the claimed system has the central computer through which the mobile application is communicated, the claimed system does not suffer from this drawback highlighted by Jansen. In fact, this section makes it clear that Jansen is describing a mobile application system in which each host platform performs its own security. Thus, Section 4.2 of Jansen does not in any way disclose or suggest a system with a central computer that performs security monitoring. Thus, Jansen does not teach this element of Claim 20.

Furthermore, Jansen does not disclose "wherein the security monitoring further comprises preventing untrusted hosts from initially launching mobile applications" as set forth in the claim. The Examiner points out that "a non-trusting host launching a mobile application reads on hostile code" in his rejection. Even assuming that the above statement is correct (which it is not), it is unclear how Jansen therefore discloses that the central computer prevents untrusted hosts from initially launching mobile applications. At most, Jansen describes the Aglet system that blocks an incoming mobile application which is very different from preventing untrusted hosts from initially launching mobile applications as set forth above. Thus, Jansen does not disclose this feature and therefore Claim 20 is allowable over Jansen.

Claim 21 is allowable over Jansen for at least the same reasons as Claim 20.

CONCLUSION

In view of the above, it is respectfully submitted that Claims 1-21 are allowable over the prior art cited by the Examiner and early allowance of these claims and the application is respectfully requested.

The Examiner is invited to call Applicant's attorney at the number below in order to speed the prosecution of this application.

The Commissioner is authorized to charge any deficiencies in fees and credit any overpayment of fees to Deposit Account No. 07-1896.

Respectfully submitted,

GRAY CARY WARE & FREIDENRICH LLP

Dated: March 31, 2004 By _____

Timothy W. Lohse
Reg. No. 35,255
Attorney for Applicant

GRAY CARY WARE & FREIDENRICH
2000 University Avenue
East Palo Alto, CA 94303
Telephone: (650) 833-2055

Gray Cary\EM\7162307.1
1010722-991101

Gray Cary\EM\7162307.1
1010722-991101